Intrinsic complexity estimates in polynomial optimization [1]

Bernd Bank [2]· Marc Giusti [3]· Joos Heintz [4]· Mohab Safey El Din [5]

April 19, 2013

Abstract

It is known that point searching in basic semialgebraic sets and the search for globally minimal points in polynomial optimization tasks can be carried out using $(s\,d)^{O(n)}$ arithmetic operations, where n and s are the numbers of variables and constraints and d is the maximal degree of the polynomials involved.

We associate to each of these problems an intrinsic system degree which becomes in worst case of order $(n\,d)^{O(n)}$ and which measures the intrinsic complexity of the task under consideration.

We design non-uniformly deterministic or uniformly probabilistic algorithms of intrinsic, quasi-polynomial complexity which solve these problems.

Keywords Polynomial optimization · Intrinsic complexity · Degree of varieties

Mathematics Subject Classification (2010) 14P10 · 14M10 · 68Q25 · 68W30

1. Research partially supported by the following Argentinian, French and Spanish grants: CONICET PIP 2461/01, UBACYT 20020100100945, PICT–2010–0525, Digiteo DIM 2009–36HD "Magix", ANR-2010-BLAN-0109-04 "LEDA", GeoLMI, ANR 2011 BS03 011 06, EXACTA, ANR-09-BLAN-0371-01, MTM2010-16051.

2. Humboldt-Universität zu Berlin, Institut für Mathematik, 10099 Berlin, Germany.
bank@mathematik.hu-berlin.de

3. CNRS, Lab. LIX, École Polytechnique, 91228 Palaiseau CEDEX, France.
Marc.Giusti@Polytechnique.fr

4. Departamento de Computación, Universidad de Buenos Aires and CONICET, Ciudad Univ., Pab.I, 1428 Buenos Aires, Argentina, and Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, 39071 Santander, Spain.
joos@dc.uba.ar

5. UPMC, Univ. Paris 06; Institut Universitaire de France; INRIA Paris Rocquencourt, POLSYS Project; CNRS, UMR digiteo dim 2009-36hd7606; LIP6 Case 169, 4, Place Jussieu, F-75252 Paris, France.
Mohab.Safey@lip6.fr

1 Introduction

We develop uniform bounded error probabilistic and non–uniform deterministic algorithms of intrinsic, quasi-polynomial complexity for the point searching problem in basic semialgebraic sets and for the search of isolated local and global minimal points in polynomial optimization. The semialgebraic sets and optimization problems have to satisfy certain well motivated geometric restrictions which allow to associate with them an intrinsic *system degree* (see Section 3.2) which controls the complexity of our algorithms and constitute the core of their intrinsic character. The algorithms we are going to design will become then polynomial in the length of the extrinsic description of the problem under consideration and its system degree (we take only arithmetic operations and comparisons in $\mathbb{Q}$ into account at unit costs). The idea is that the system degree constitutes a geometric invariant which measures the intrinsic "complexity" of the *concrete* problem under consideration (not of all problems like a worst case complexity). In worst case the sequential time complexity will be of order $\binom{s}{p}(n\,d)^{O(n)}$ or $(n\,d)^{O(n)}$, where n is the number of variables and d the maximal degree of the polynomials occurring in the problem description, s their number and $1 \leq p \leq n$ the maximal codimension of the real varieties given by the active constraints. We shall suppose that these polynomials are represented as outputs of an essentially division–free arithmetic circuit in $\mathbb{Q}[X_1, \ldots, X_n]$ of size L (here, we mean by essentially division-free that only divisions by rational numbers are allowed). The (sequential) complexity of our algorithms is then of order $L\binom{s}{p}n^{O(p)}d^{O(1)}\delta^2$ (or $L(n\,d)^{O(1)}\delta^2$), where δ is the intrinsic system degree which in worst case becomes of order $(s\,n\,d)^{O(n)}$ (or $(n\,d)^{O(n)}$). We call this type of complexity bounds *intrinsic* and *quasi-polynomial*.

For the problem of deciding the consistency of a given set of inequality constraints and to find, in case the answer is positive, a real algebraic sample point for each connected component of the corresponding semialgebraic set sequential time bounds of order $(sd)^{O(n)}$, $(sd)^{O(n^2)}$ and $(sd)^{O(n^3)}$ are exhibited in [24, 12, 34, 27, 35, 7, 29] and in the book [8]. Such bounds can also be derived from efficient quantifier elimination algorithms over the reals ([27, 35, 7, 8]). Since two alternating blocks of quantifiers become involved, one would expect at first glance that only a $(sd)^{O(n^2)}$ time complexity bound could be deduced from efficient real quantifier elimination for polynomial optimization problems. But, at least for global optimization, one can do much better with an $s^{2n+1}d^{O(n)}$ sequential time bound (see [8], Algorithm 14.46, the result is essentially due to [35]). For particular global polynomial optimization problems the constant hidden in this bound can be made precise and the algorithms become implementable (see [22, 38, 37] and [21]). Accurate estimations for the minima are contained in [29].

Nevertheless, this article does not focus on the improvement of known worst case complexity bounds in optimization theory. Our aim is to exhibit large classes of point searching problems in semialgebraic sets and polynomial optimization problems where it makes sense to speak about intrinsic complexity of solution algorithms. This is the reason why we put the accent on geometrical aspects of these problems. The algorithms become then borrowed from [20] (see also [18, 19, 26, 15, 11]) and, in particular, from [2, 3] (or alternatively from [36]).

It is not straightforward but possible to transfer our algorithms and complexity results to the bit model. The main task of such a transfer concerns the algorithms from [2, 3] we use and this exceeds the scope of this paper.

1.1 Notions and Notations

We shall freely use standard notions, results and notations from algebraic and semialgebraic geometry, commutative algebra and algebraic complexity theory which can be found e.g. in the books [32, 39, 33, 10].

Let $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ be the fields of the rational, real and complex numbers, respectively, let $X_1, \ldots, X_n$ be indeterminates over $\mathbb{C}$ and let $F_1, \ldots, F_p$ be a regular sequence of polynomials in $\mathbb{R}[X_1, \ldots, X_n]$ defining a closed, $\mathbb{R}$–definable subvariety S of the n–dimensional complex affine space $\mathbb{C}^n$. Thus S is a nonempty equidimensional affine variety of dimension $n-p$, i.e., each irreducible component of S is of dimension $n-p$. We denote by $S_{\mathbb{R}} := S \cap \mathbb{R}^n$ the real trace of the complex variety S. We shall use also the following notations:

$$\{F_1 = 0, \ldots, F_p = 0\} := S \text{ and } \{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}} := S_{\mathbb{R}}.$$

For a given polynomial $G \in \mathbb{R}[X_1, \ldots, X_n]$ we denote by S_G and $(S_{\mathbb{R}})_G$ the sets of points of S and $S_{\mathbb{R}}$ at which G does not vanish.

We call the regular sequence $F_1, \ldots, F_p$ *reduced* if for any index $1 \leq k \leq p$ the ideal $(F_1, \ldots, F_k)$ is radical. A point x of $\mathbb{C}^n$ is called $(F_1, \ldots, F_p)$*–regular* if the Jacobian $J(F_1, \ldots, F_p) := \left[\frac{\partial F_j}{\partial X_k}\right]_{\substack{1 \leq j \leq p \\ 1 \leq k \leq n}}$ has maximal rank p at x. Observe, that for each *reduced* regular sequence $F_1, \ldots, F_p$ defining the variety S, the locus of $(F_1, \ldots, F_p)$–regular points of S is the same. In this case we call an $(F_1, \ldots, F_p)$–regular point of S simply *regular* (or *smooth*) or we say that S is regular (or smooth) at x. The variety S is called $(F_1, \ldots, F_p)$–regular or smooth if S is $(F_1, \ldots, F_p)$–regular at any of its points.

For a given affine variety V denote by $\mathbb{C}[V]$ its coordinate ring. We call the elements of $\mathbb{C}[V]$ coordinate functions. For $g \in \mathbb{C}[V]$ we denote by $\mathbb{C}[V]_g$ the localization of $\mathbb{C}[V]$ at g. Observe that $\mathbb{C}[V]_g$ is isomorphic to $\mathbb{C}[V_g]$.

Suppose for the moment that V is a closed subvariety of $\mathbb{C}^n$. For V irreducible we define its degree $\deg V$ as the maximal number of points we can obtain by cutting V with finitely many affine hyperplanes of $\mathbb{C}^n$ such that the intersection is finite. Observe that this maximum is reached when we intersect V with dimension of V many *generic* affine hyperplanes of $\mathbb{C}^n$. In case that V is not irreducible let $V = C_1 \cup \cdots \cup C_s$ the decomposition of V into irreducible components. We define the degree of V as $\deg V := \sum_{1 \leq j \leq s} \deg C_j$.

With this definition we can state the so-called *Bézout Inequality*:

Let V and W be closed subvarieties of $\mathbb{C}^n$. Then we have

$$\deg(V \cap W) \leq \deg V \cdot \deg W.$$

If V is a hypersurface of $\mathbb{C}^n$ then its degree equals the degree of its minimal equation. The degree of a point of $\mathbb{C}^n$ is just one. For more details we refer to [25, 16, 40].

Let $1 \leq i \leq n-p$ and let $a := [a_{k,l}]_{\substack{1\leq k\leq n-p-i+1\\ 0\leq l\leq n}}$ be a real $((n-p-i+1)\times(n+1))$–matrix with $(a_{10},\ldots,a_{n-p-i+1,0}) \neq 0$ and suppose that $[a_{k,l}]_{\substack{1\leq k\leq n-p-i+1\\ 1\leq l\leq n}}$ has maximal rank $n-p-i+1$.

The dual ith polar variety of S associated with the matrix a is defined as closure of the locus of the $(F_1,\ldots,F_p)$–regular points of S where all $(n-i+1)$–minors of the polynomial $((n-i+1)\times n)$–matrix

$$\begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_n} \\ a_{1,1}-a_{1,0}X_1 & \cdots & a_{1,n}-a_{1,0}X_n \\ \vdots & \vdots & \vdots \\ a_{n-p-i+1,1}-a_{n-p-i+1,0}X_1 & \cdots & a_{n-p-i+1,n}-a_{n-p-i+1,0}X_n \end{bmatrix}$$

vanish.

Observe that this definition of dual polar varieties may be extended to the case that there is given a Zariski open subset O of $\mathbb{C}^n$ such that the equations $F_1=0,\ldots,F_p=0$ intersect transversally at any of their common solutions in O and that S is now the locally closed subvariety of $\mathbb{C}^n$ given by

$$S := \{F_1=0,\ldots,F_p=0\}\cap O.$$

In [2] and [3] we have introduced the notion of dual polar variety of S and motivated by geometric arguments the calculatory definition above of these objects. Moreover, we have shown that, for a real $((n-p-i+1)\times(n+1))$–matrix $a=[a_{k,l}]_{\substack{1\leq k\leq n-p-i+1\\ 0\leq l\leq n}}$ with $[a_{k,l}]_{\substack{1\leq k\leq n-p-i+1\\ 1\leq l\leq n}}$ *generic*, the ith polar varieties is either empty or of pure codimension i in S. Further, we have shown that this polar variety is normal and Cohen–Macaulay (but not necessarily smooth) at any of their $(F_1,\ldots,F_p)$–regular points (see [4], Corollary 2 and Section 3.1). This motivates the consideration of the so–called *generic* dual polar varieties associated with real $((n-p-i+1)\times(n+1))$–matrices a which are generic in the above sense, as invariants of the variety S (independently of the given equation system $F_1=0,\ldots,F_p=0$).

For our use of the word "generic" we refer to [4], Definition 1.

In case that $S_{\mathbb{R}}$ is smooth and a is a real $((n-p-i+1)\times(n+1))$–matrix, as before, the ith dual polar variety associated with a contains at least one point of each connected component of $S_{\mathbb{R}}$ and is therefore not empty (see [2] and [3], Proposition 2).

2 Inequalities

Let $F_1,\ldots,F_s \in \mathbb{R}[X_1,\ldots,X_n]$ and $1 \leq p \leq \min\{s,n\}$. We assume that for any $1\leq j_1<\cdots<j_k\leq s$, $1\leq k\leq p$ the following condition is satisfied.

Condition A

The polynomials $F_{j_1}, \ldots, F_{j_k}$ *generate in* $\mathbb{R}[X_1, \ldots, X_n]$ *the trivial ideal or form a reduced regular sequence and the semialgebraic set* $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}}$ *is empty or* $(F_{j_1}, \ldots, F_{j_k})$*–regular. Moreover, any* $p+1$ *polynomials of* $F_1, \ldots, F_s$ *have no common real zero.*

For $\varepsilon_1, \ldots, \varepsilon_s \in \{-1, 1\}$ let

$$\{\operatorname{sign} F_1 = \varepsilon_1, \ldots, \operatorname{sign} F_s = \varepsilon_s\} := \{x \in \mathbb{R}^n \mid \operatorname{sign} F_1(x) = \varepsilon_1, \ldots, \operatorname{sign} F_s(x) = \varepsilon_s\}.$$

From now on we shall suppose without loss of generality $\varepsilon_1 = \cdots = \varepsilon_s = 1$ and write

$$\{F_1 > 0, \ldots, F_s > 0\} \text{ instead of } \{\operatorname{sign} F_1(x) = 1, \ldots, \operatorname{sign} F_s(x) = 1\}.$$

Let us fix a maximal index set $1 \leq j_1 < \cdots < j_k \leq s,\ 1 \leq k \leq p$ with

$$\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}} \cap \overline{\{F_1 > 0, \ldots, F_s > 0\}} \neq \emptyset.$$

Lemma 1

$$\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}} \cap \overline{\{F_1 > 0, \ldots, F_s > 0\}} = \\ = \{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}} \cap \{F_j > 0,\ 1 \leq j \leq s,\ j \neq j_1, \ldots, j \neq j_k\}.$$

Proof. We show first the inclusion of the left hand side of the set equation in the right hand side. For this purpose, let x be an arbitrary point of $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}} \cap \overline{\{F_1 > 0, \ldots, F_s > 0\}}$. Suppose that there exists an index $1 \leq j \leq s,\ j \neq j_1, \ldots, j \neq j_k$ with $F_j(x) = 0$. Then x belongs to $\{F_{j_1} = 0, \ldots, F_{j_k} = 0, F_j = 0\}_{\mathbb{R}} \cap \overline{\{F_1 > 0, \ldots, F_s > 0\}}$ which by the maximal choice of $1 \leq j_1 < \cdots < j_k \leq s$ is empty. Therefore, we have $F_j(x) \neq 0$ for any index $1 \leq j \leq s,\ j \neq j_1, \ldots, j \neq j_k$. Since x belongs to $\overline{\{F_1 > 0, \ldots, F_s > 0\}}$, we have $F_j(x) > 0$.
We are now going to show the inverse inclusion. Consider an arbitrary point $x \in \{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}} \cap \{F_j > 0,\ 1 \leq j \leq s,\ j \neq j_1, \ldots, j \neq j_k\}$ and let U be an arbitrary neighborhood of x in $\mathbb{R}^n$. Without loss of generality we may assume that U is contained in $\{F_j > 0,\ 1 \leq j \leq s,\ j \neq j_1, \ldots, j \neq j_k\}$. Since by Condition A the point x is contained in the $(F_{j_1}, \ldots, F_{j_k})$–regular set $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}}$, the polynomial map from $\mathbb{R}^n$ into $\mathbb{R}^n$ given by $(F_{j_1}, \ldots, F_{j_k})$ is a submersion at x and therefore there exists a point $y \in U$ with $F_{j_1}(y) > 0, \ldots, F_{j_k}(y) > 0$. Because U was an arbitrary neighborhood of x, we conclude that x belongs to $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}} \cap \overline{\{F_1 > 0, \ldots, F_s > 0\}}$. □

Corollary 2
Let C *be a connected component of* $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}}$ *with* $C \cap \overline{\{F_1 > 0, \ldots, F_s > 0\}} \neq \emptyset$. *Then*

$$C \subset \{F_j > 0,\ 1 \leq j \leq s,\ j \neq j_1, \ldots, j \neq j_k\}.$$

Proof. Lemma 1 implies that the set

$$\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}} \cap \overline{\{F_1 > 0, \ldots, F_s > 0\}}$$

is open and closed in $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}}$. Therefore this set is the union of all the connected components of $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}}$ which have a nonempty intersection with $\overline{\{F_1 > 0, \ldots, F_s > 0\}}$. This implies Corollary 2. □

2.1 Converting nonstrict inequalities into strict ones

Let $1 \leq k \leq p$, $1 \leq j_1 < \cdots < j_k \leq s$ and let $x = (x_1, \ldots, x_n)$ be a point of $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}} \cap \{F_1 > 0, \ldots, F_s > 0\}$. Thus x satisfies the system of nonstrict inequalities

$$F_{j_1}(x) \geq 0, \ldots, F_{j_k}(x) \geq 0, \;\; F_j(x) > 0, \; 1 \leq j \leq s, \; j \neq j_1, \ldots, j \neq j_k$$

Starting from x we wish to construct a point $y \in \mathbb{R}^n$ which satisfies the strict inequalities

$$F_j(y) > 0, \; 1 \leq j \leq s.$$

From Condition A we conclude that the Jacobian $J(F_{j_1}, \ldots, F_{j_k})$ has full rank k at x. Therefore we may efficiently find a vector $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{R}^n$ such that the entries of $J(F_{j_1}, \ldots, F_{j_k})(x)\mu^T$ are all positive (here, μ^T denotes the transposed vector of μ).

Let Y be a new indeterminate and for $1 \leq j \leq s$ let $G_j := F_j(\mu_1 Y + x_1, \ldots, \mu_n Y + x_n)$. Observe, that the univariate polynomial G_j satisfies the equation $\frac{dG_j}{dY}(0) = \sum_{1 \leq i \leq n} \frac{\partial F_j}{\partial X_i}(x)\mu_i$. In particular, the entries of

$$(\frac{dG_{j_1}}{dY}(0), \ldots, \frac{dG_{j_k}}{dY}(0)) = J(F_{j_1}, \ldots, F_{j_k})(x)\mu^T$$

are all positive. Let $c > 0$ be the smallest positive zero of $\prod_{1 \leq j \leq s} G_j$ (if there exists none, c may be any positive real number). Then one verifies immediately that $z := x + \frac{c}{2}\mu$ satisfies for any index $1 \leq j \leq s$ the condition $F_j(z) = G_j(\frac{c}{2}) > 0$.

2.2 Finding sample points for all consistent sign conditions

Let $(\varepsilon_1, \ldots, \varepsilon_s) \in \{-1, 0, 1\}^s$. The polynomial inequality system $\operatorname{sign} F_1 = \varepsilon_1, \ldots, \operatorname{sign} F_s = \varepsilon_s$ is called a *sign condition* on $F_1, \ldots, F_s$ which we say to be *consistent* if there exists a point $x \in \mathbb{R}^n$ satisfying it. In case $(\varepsilon_1, \ldots, \varepsilon_s) \in \{-1, 1\}^s$ we call the sign condition *strict*, otherwise *nonstrict*. A real algebraic point of $\mathbb{R}^n$ which is supposed to be encoded "à la Thom" [13] and to satisfy the sign condition is called a *sample point* of it .

Let $F_1, \ldots, F_s$ be given as outputs of an essentially division–free arithmetic circuit β in $\mathbb{Q}[X_1, \ldots, X_n]$ having size L and non–scalar depth ℓ (hence, $F_1, \ldots, F_s$ belong to $\mathbb{Q}[X_1, \ldots, X_n]$). Let $d \geq 2$ be an upper bound of $\deg F_1, \ldots, \deg F_s$. For $1 \leq k \leq p$

and $1 \leq j_1 < \cdots < j_k \leq s$ let $\delta_{j_1,\ldots,j_k}$ be the maximal degree of $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}$ and all generic dual polar varieties of this variety. Let finally

$$\delta := \max\{\delta_{j_1,\ldots,j_k} \mid 1 \leq j_1 < \cdots < j_k \leq s,\ 1 \leq k \leq p\}.$$

We call δ the *degree* of the sample point finding problem for all consistent sign conditions of $F_1, \ldots, F_s$. From the Bézout Inequality we deduce $\delta \leq p^{n-p} d^n$. Using the algorithms from [2, 3] (see also [5] for technical details) we construct for each $1 \leq k \leq p$ and $1 \leq j_1 < \cdots < j_k \leq s$ real algebraic sample points for each connected component of $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}}$. Then we evaluate the signs of all $F_j,\ 1 \leq j \leq s\ j \neq j_1, \ldots, j \neq j_k$ on these sample points. In this way we obtain sample points for all nonstrict consistent sign conditions on $F_1, \ldots, F_s$. As far as only sample points for the strict sign conditions on $F_1, \ldots, F_s$ are required, we limit our attention to sample points of the connected component of $\{F_{j_1} = 0, \ldots, F_{j_k} = 0\}_{\mathbb{R}}$ where the signs of all $F_j, 1 \leq j \leq s\ \ j \neq j_1, \ldots, j \neq j_k$ are all strict. Let x be such a sample point with $\operatorname{sign} F_j(x) = \varepsilon_j$, and $\varepsilon_j \in \{-1, 1\}$ for $1 \leq j \leq s$ with $j \neq j_1, \ldots, j \neq j_k$. Then, following Subsection 2.1, for any $\varepsilon_{j_1}, \ldots, \varepsilon_{j_k} \in \{-1, 1\}$ we may convert x into a real algebraic sample point of the strict sign conditions $\operatorname{sign} F_1 = \varepsilon_1, \ldots, \operatorname{sign} F_s = \varepsilon_s$. The whole procedure can be realized in time $L\binom{s}{p} n^{O(p)} d^{O(1)} \delta^2$ (here arithmetic operations and comparisons in $\mathbb{Q}$ are taken into account at unit costs). We have therefore shown the following statement which constitutes a simplified variant of [31], Theorem 5.

Theorem 3
Let n, d, p, s, L, ℓ, $\delta \in \mathbb{N}$ with $1 \leq p \leq n$ be arbitrary and let $F_1, \ldots, F_s \in \mathbb{Q}[X_1, \ldots, X_n]$ be polynomials of degree at most d satisfying Condition A and having sample point finding degree at most δ. Suppose that $F_1, \ldots, F_s$ are given as outputs of an essentially division-free circuit β in $\mathbb{Q}[X_1, \ldots, X_n]$ of size L.

There exists a uniform bounded error probabilistic algorithm $\mathcal{A}$ over $\mathbb{Q}$ which computes from the input β in time $L\binom{s}{p} n^{O(p)} d^{O(1)} \delta^2 = s^{O(p)}(nd)^{O(n)}$ real algebraic sample points for each consistent sign condition on $F_1, \ldots, F_s$ (here, algebraic operations and comparisons in $\mathbb{Q}$ are taken into account at unit costs).

For any n, d, p, s, L, ℓ, $\delta \in \mathbb{N}$ with $1 \leq p \leq n$ the probabilistic algorithm $\mathcal{A}$ may be realized by an algebraic computation tree of depth $L\binom{s}{p} n^{O(p)} d^{O(1)} \delta^2 = s^{O(p)}(n\,d)^{O(n)}$ that depends on parameters which may be chosen randomly.

Observe that in the elimination process which leads to Theorem 3, the intermediate polynomials may become of degree $nd\delta$. Thus δ is not an upper bound for them.

3 Optimization

We associate with a polynomial optimization problem with smooth equality constraints certain natural geometric conditions and an intrinsic invariant that controls the complexity of the algorithm which we are going to develop in order to solve this problem. Our approach has some features in common with that of [23].

3.1 Geometric considerations

Let be given polynomials $G, F_1, \ldots, F_p \in \mathbb{R}[X_1, \ldots, X_n]$, $1 \leq p \leq n$, and suppose that $F_1, \ldots, F_p$ form a reduced regular sequence and that the real trace $V_{\mathbb{R}}$ of

$$V := \{x \in \mathbb{C}^n \mid F_1(x) = 0, \ldots, F_p(x) = 0\}$$

is nonempty and smooth.
For $1 \leq j_1 < \cdots < j_p \leq n$ denote by $\Delta_{j_1,\ldots,j_p}$ the p–minor of the Jacobian $J(F_1, \ldots, F_p)$ given by the columns numbered $j_1, \ldots, j_p$ and by

$$M_1^{(j_1,\ldots,j_p)}, \ldots, M_{n-p}^{(j_1,\ldots,j_p)}$$

the $(p+1)$–minors of $((p+1) \times n)$–matrix

$$\begin{bmatrix} J(F_1, \ldots, F_p) \\ \frac{\partial G}{\partial X_1} \cdots \frac{\partial G}{\partial X_n} \end{bmatrix}$$

given by the columns numbered $j_1, \ldots, j_p$ to which we add, one by one, the columns numbered by the indices belonging to the set $\{1, \ldots, n\} \setminus \{j_1, \ldots, j_p\}$.
Let x be a local minimal point of G on $V_{\mathbb{R}}$. Then the Karush-Kuhn-Tucker conditions imply that $\operatorname{rk} \begin{bmatrix} J(F_1, \ldots, F_p) \\ \frac{\partial G}{\partial X_1} \cdots \frac{\partial G}{\partial X_n} \end{bmatrix} (x) \leq p$ holds. Let

$$W := \{x \in V \mid \operatorname{rk} \begin{bmatrix} J(F_1, \ldots, F_p) \\ \frac{\partial G}{\partial X_1} \cdots \frac{\partial G}{\partial X_n} \end{bmatrix} (x) \leq p\}$$

and let $1 \leq j_1 < \cdots < j_p \leq n$. Then we deduce from the Exchange Lemma in [1] that

$$W_{\Delta_{j_1,\ldots,j_p}} = V_{\Delta_{j_1,\ldots,j_p}} \cap \{M_1^{(j_1,\ldots,j_p)}(x) = 0, \ldots, M_{n-p}^{(j_1,\ldots,j_p)}(x) = 0\}$$

holds.
From now on we assume that G and $F_1, \ldots, F_p$ satisfy the following three conditions for any $1 \leq j_1 < \cdots < j_p \leq n$ and any $1 \leq k \leq n - p$.

Let D_k denote the union of all irreducible components of W of dimension strictly larger than $n - p - k$. Observe that D_{n-p+1} is also well defined.

Condition B
Any point of

$$\Big((V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}} \cap \{M_1^{(j_1,\ldots,j_p)}(x) = 0, \ldots, M_k^{(j_1,\ldots,j_p)}(x) = 0\}_{\mathbb{R}}\Big) \setminus (D_k)_{\mathbb{R}}$$

is $(F_1, \ldots, F_p, M_1^{(j_1,\ldots,j_p)}, \ldots, M_k^{(j_1,\ldots,j_p)})$ *–regular.*

Condition B implies that the real trace of $V_{\Delta_{j_1,\ldots,j_p}} \cap \{M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}$ is smooth. Let $C_1, \ldots, C_s$ be the irreducible components of

$$(V_{\Delta_{j_1,\ldots,j_p}} \cap \{M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}) \setminus D_k.$$

Condition C
For any $1 \leq j \leq s$ *the semialgebraic set*

$$(C_j)_{\mathbb{R}} \setminus (C_1 \cup \cdots \cup C_{j-1} \cup C_{j+1} \cup \cdots \cup C_s)_{\mathbb{R}}$$

is dense in $(C_j)_{\mathbb{R}}$ *and* $(C_j)_{\mathbb{R}}$ *is nonempty.*

Condition C implies that each irreducible component of W contains a real point, that $(C_1)_{\mathbb{R}}, \ldots, (C_s)_{\mathbb{R}}$ are the irreducible components of the real trace of $(V_{\Delta_{j_1,\ldots,j_p}} \cap \{M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}) \setminus D_k$ and that $C_1, \ldots, C_s$ can be obtained from the complex interpretation of the defining equations of $(C_1)_{\mathbb{R}}, \ldots, (C_s)_{\mathbb{R}}$.

Condition D
The polynomial $\Delta_{j_1,\ldots,j_p}$ *does not vanish identically on any irreducible component of* $V \cap \{M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}$.

We need Condition D only for the proof of Lemma 6 below. We may therefore replace Condition D by the statement of Lemma 6. Condition D is the less intuitive one of our conditions. We need it to make the algorithm in Section 3.2 work correctly.

Lemma 4
Let notations be as before. For any $1 \leq j \leq s$ *we have* $\dim C_j = \dim(C_j)_{\mathbb{R}} = n-p-k$.

Proof. Since $(C_j)_{\mathbb{R}}$ is nonempty there exists by Condition C an open semialgebraic subset U of $\mathbb{R}^n$, disjoint from $(D_k \cup C_1 \cup \cdots \cup C_{j-1} \cup C_{j+1} \cup \cdots \cup C_s)_{\mathbb{R}}$, with $U \cap (C_j)_{\mathbb{R}} \neq \emptyset$. This implies

$$U \cap (V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}} \cap \{M_1^{(j_1,\ldots,j_p)}(x) = 0, \ldots, M_k^{(j_1,\ldots,j_p)}(x) = 0\}_{\mathbb{R}} = U \cap (C_j)_{\mathbb{R}}.$$

From $U \cap D_k = \emptyset$ and Condition B we infer now that any point of the semialgebraic set $U \cap (C_j)_{\mathbb{R}}$ is $(F_1, \ldots, F_p, M_1^{(j_1,\ldots,j_p)}, \ldots, M_k^{(j_1,\ldots,j_p)})$–regular. Hence, $\dim C_j = \dim(C_j)_{\mathbb{R}} = n - p - k$. □

Lemma 5
Let C *be an irreducible component of* W. *Then* G *takes a constant real value on* C.

Proof. Since by assumption $V_{\mathbb{R}} = \{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$ is smooth and since $C_{\mathbb{R}}$ is nonempty by Condition C, there exist indices $1 \leq j_1 < \cdots < j_p \leq n$ with $(C_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}} \neq \emptyset$. Furthermore, there exists an index $1 \leq k \leq n - p$ with $\dim C = n - p - k$.
From now on let notations be as before. Without loss of generality we may assume that $C_{\Delta_{j_1,\ldots,j_p}} \setminus D_k = C_1$ holds. By Condition C the semialgebraic set $(C_1)_{\mathbb{R}} \setminus (C_2 \cup \cdots \cup C_s)_{\mathbb{R}}$ is nonempty. Let x be an arbitrary point of this set. As we have seen in the proof of Lemma 4, there exists an open semialgebraic neighborhood U of x in $\mathbb{R}^n$ with

$$U \cap (V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}} \cap \{M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}_{\mathbb{R}} = U \cap (C_1)_{\mathbb{R}}$$

and $U \cap (D_k)_{\mathbb{R}} = \emptyset$. Condition B implies now that $U \cap (C_1)_{\mathbb{R}}$ is a smooth semialgebraic manifold which we may suppose to be connected by continuously differentiable paths.

Let y be an arbitrary point of $U \cap (C_1)_{\mathbb{R}}$ and let τ be a continuously differentiable path in $U \cap (C_1)_{\mathbb{R}}$ that connects x with y. We may suppose that τ can be extended to a suitable open neighborhood of $[0,1]$ in $\mathbb{R}$ and that $\tau(0) = x$ and $\tau(1) = y$ holds. Observe that $\tau([0,1])$ is contained in $V_{\mathbb{R}}$. The path τ depends on a parameter T defined in the given neighborhood of $[0,1]$. Let $\tau(T) := (\tau_1(T), \ldots, \tau_n(T))$. Since $\tau([0,1])$ is contained in $V_{\mathbb{R}}$ the vector $(\frac{d\tau_1}{dT}(t), \ldots, \frac{d\tau_n}{dT}(t))$ belongs to the kernel of $J((F_1, \ldots, F_p))(\tau(t))$ for any $t \in [0,1]$. On the other hand, $C_1 \subset C \subset W$ implies that $(\frac{\partial G}{\partial X_1}(\tau(t)), \ldots, \frac{\partial G}{\partial X_n}(\tau(t))$ is linearly dependent on the full rank matrix $J(F_1, \ldots, F_p)(\tau(t))$. Therefore we have $\frac{d(G \circ \tau)}{dT}(t) = \sum_{i=1}^{n} \frac{\partial G}{\partial X_i}(\tau(t)) \frac{d\tau_i}{dT}(t) = 0$ for any $t \in [0,1]$. Hence, $G \circ \tau$ is constant on $[0,1]$. Consequently, we have $G(x) = G(\tau(0)) = G(\tau(1)) = G(y)$. From the arbitrary choice of x and y in $U \cap (C_1)_{\mathbb{R}}$ we infer that G takes on $U \cap (C_1)_{\mathbb{R}}$ a constant value. Thus the restriction of G to the semialgebraic set $(C_1)_{\mathbb{R}} \setminus (C_2 \cup \cdots \cup C_s)_{\mathbb{R}}$ is locally constant and takes therefore only finitely many values in $\mathbb{R}$. Condition C implies now that the same is true for the restriction of G to $(C_1)_{\mathbb{R}}$.

By Conditions B and C there exists an $(F_1, \ldots, F_p, M_1^{(j_1,\ldots,j_p)}, \ldots, M_k^{(j_1,\ldots,j_p)})$–regular point $x = (x_1, \ldots, x_n)$ of $(C_1)_{\mathbb{R}} \setminus (C_2 \cup \cdots \cup C_s)_{\mathbb{R}}$. Hence, there exists an open semialgebraic neighborhood U of x in $\mathbb{R}^n$ and $n-p-k$ parameters $\xi_1, \ldots, \xi_{n-p-k}$ of $U \cap C_1$ such that the restriction of G to $U \cap (C_1)_{\mathbb{R}}$ can be developed into a convergent power series $P(\xi_1 - x_1, \ldots, \xi_{n-p-k} - x_{n-p-k})$ around $(x_1, \ldots, x_{n-p-k})$. Since G is locally constant on $U \cap (C_1)_{\mathbb{R}}$ we conclude that $P(\xi_1 - x_1, \ldots, \xi_{n-p-k} - x_{n-p-k})$ equals its constant term, say $b \in \mathbb{R}$.

On the other hand, there exists an open neighborhood O of x in $\mathbb{C}^n$ such that the restriction of G to $O \cap C_1$ can be developed into a convergent power series in $\xi_1 - x_1, \ldots, \xi_{n-p-k} - x_{n-p-k}$. This power series must necessarily be $P(\xi_1 - x_1, \ldots, \xi_{n-p-k} - x_{n-p-k})$. Thus G takes on $O \cap C_1$ only the real value b. Suppose that G takes on C_1 a value different from b. Then $(C_1)_{G-b}$ is nonempty and therefore (by [32], Ch. I, Section 10, Corollary 1) dense in the Euclidean topology of C_1. In particular, there exists a point $y \in O \cap C_1$ with $G(y) \neq b$. This contradiction implies Lemma 5. □

Let $1 \leq k \leq n-p$. By Lemma 5 the polynomial G takes on D_k only finitely many values which are all real. Denote by B_k the set of these values and let $R_k := \prod_{b \in B_k}(G - b)$. Observe that R_k belongs to $\mathbb{R}[X_1, \ldots, X_n]$ and that B_{n-p+1} is well defined.

Lemma 6
For any $1 \leq j_1 < \cdots < j_p \leq n$ and $1 \leq k \leq n-p$ the polynomials $(F_1, \ldots, F_p, M_1^{(j_1,\ldots,j_p)}, \ldots, M_k^{(j_1,\ldots,j_p)})$ generate the trivial ideal or form a reduced regular sequence in $\mathbb{R}[X_1, \ldots, X_n]_{R_k}$.

Proof. Fix $1 \leq j_1 < \cdots < j_p \leq n$. By Condition D it suffices to prove that for any $1 \leq k \leq n-p$ the polynomials $(F_1, \ldots, F_p, M_1^{(j_1,\ldots,j_p)}, \ldots, M_k^{(j_1,\ldots,j_p)})$ define in $\mathbb{C}^n_{\Delta_{j_1,\ldots,j_p} \cdot R_k}$ an equidimensional variety of dimension $n-p-k$ and, that each irreducible component of this variety contains an $(F_1, \ldots, F_p, M_1^{(j_1,\ldots,j_p)}, \ldots, M_k^{(j_1,\ldots,j_p)})$–regular

point. The first statement follows from Lemma 4 and 5, whereas the second one is a direct consequence of Conditions B and C. □

To indices $1 \leq j_1 < \cdots < j_n \leq n$ we may associate a Hessian matrix $H_{j_1,\ldots,j_p}$ of G on $V_{\Delta_{j_1,\ldots,j_p}}$ whose entries belong to $\mathbb{R}[X_1,\ldots,X_n]_{\Delta_{j_1,\ldots,j_p}}$. Let x be an arbitrary point of $V_{\Delta_{j_1,\ldots,j_p}}$. One verifies easily that the conditions $\det H_{j_1,\ldots,j_p}(x) \neq 0$ and $\det J(F_1,\ldots,F_p,M_1^{(j_1,\ldots,j_p)},\ldots,M_{n-p}^{(j_1,\ldots,j_p)})(x) \neq 0$ are equivalent.

Lemma 7
Let $1 \leq j_1 < \cdots < j_p \leq n$. The set of isolated local minimal points of G on $(V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$ is exactly the set of points of $(W_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$ where $H_{j_1,\ldots,j_p}$ is positive definite.

Proof. From Lemma 5 one deduces easily that the points of $(W_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$ where $H_{j_1,\ldots,j_p}$ is positive definite, are local minimizers of G on $(V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$. So, we have only to show that the isolated local minimal points of G in $(V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$ belong to $(W_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$ and that their Hessians are positive definite.
Let $x \in (V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$ be an isolated minimal point of G in $(V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$. Then, as we have seen, x belongs to $(W_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$. Let C be an arbitrary irreducible component of $W_{\Delta_{j_1,\ldots,j_p}}$ which contains x. Let $n-p-k$ with $1 \leq k \leq n-p$ be the dimension of C. Suppose that $1 \leq k < n-p$ holds. Conditions B and C imply now that there exists an open subset of $(F_1,\ldots,F_p,M_1^{(j_1,\ldots,j_p)},\ \ldots,M_k^{(j_1,\ldots,j_p)})$–regular points of $C_{\mathbb{R}}$ which is dense in $C_{\mathbb{R}}$. This implies that any neighborhood of x in $C_{\mathbb{R}}$ contains a point y different from x. Since $G(y) = G(x)$ holds by Lemma 5, the local minimal point x of G in $(V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$ cannot be isolated. Therefore, we have $k = n-p$. From Condition B we deduce that x is $(F_1,\ldots,F_p,M_1^{(j_1,\ldots,j_p)},\ \ldots,M_{n-p}^{(j_1,\ldots,j_p)})$–regular. Hence, $\det H_{j_1,\ldots,j_p}(x) \neq 0$. The Morse Lemma (see [14]) implies now that $H_{j_1,\ldots,j_p}(x)$ must be positive definite for x being an isolated local minimal point of G in $(V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$. □

3.1.1 Unconstrained optimization

We illustrate our argumentation in the case of unconstrained optimization. In this case we have $p := 0$ and V is the complex affine space $\mathbb{C}^n$. There is given a polynomial $G \in \mathbb{R}[X_1,\ldots,X_n]$ and the task is to characterize the local minimal points of G in $\mathbb{R}^n$. Such a local minimal point belongs to $W := \{\frac{\partial G}{\partial X_1} = 0,\ldots,\frac{\partial G}{\partial X_n} = 0\}$. For the unconstrained optimization problem we consider the following two conditions for any $1 \leq k \leq n$.
Let D_k be the union of all irreducible components of W of dimension strictly larger than $n-k$.

Condition E

Any point of $\{\frac{\partial G}{\partial X_1} = 0,\ldots,\frac{\partial G}{\partial X_k} = 0\}_{\mathbb{R}} \setminus (D_k)_{\mathbb{R}}$ is $(\frac{\partial G}{\partial X_1},\ldots,\frac{\partial G}{\partial X_k})$–regular.

Let $C_1,\ldots,C_s$ be the irreducible components of $\{\frac{\partial G}{\partial X_1} = 0,\ldots,\frac{\partial G}{\partial X_k} = 0\} \setminus (D_k)$

Condition F

For any $1 \leq j \leq s$ the semialgebraic set $(C_j)_{\mathbb{R}} \setminus (C_1 \cup \cdots \cup C_{j-1} \cup C_{j+1} \cup \cdots \cup C_s)_{\mathbb{R}}$ is dense in $(C_j)_{\mathbb{R}}$ and $(C_j)_{\mathbb{R}}$ is non empty.

If these conditions are satisfied by G we can prove in the same way as in case of Lemma 4, 5, 6 and 7 the following corresponding statements.

Lemma 8
Let notations be as before. For any $1 \leq j \leq s$, *we have* $\dim C_j = \dim(C_j)_{\mathbb{R}} = n - k$.

Lemma 9
Let C *be an irreducible component of* W. *Then* G *takes a constant value on* C.

Let $1 \leq k \leq n$. By Lemma 9 the polynomial G takes on D_k only finitely many values which are all real. Denote by B_k the set of these values and let $R_k := \prod_{b \in B_k}(G - b) \in \mathbb{R}[X_1, \ldots, X_n]$.

Lemma 10
For any $1 \leq k \leq n$, *the polynomials* $\frac{\partial G}{\partial X_1}, \ldots, \frac{\partial G}{\partial X_k}$ *form a reduced regular sequence in* $\mathbb{R}[X_1, \ldots, X_n]_{R_k}$.

Lemma 11
The set of isolated local minimal points of G *in* $\mathbb{R}^n$ *is exactly the set of points of* $W_{\mathbb{R}}$ *where the Hessian of* G *is positive definite.*

3.2 Algorithms

Let notations and assumptions be as in the previous subsection. We associate with G and $F_1, \ldots, F_p$ intrinsic invariants that control the complexity of the algorithms we are going to develop in order to solve the computational problems of minimizing locally and globally G on the set of points in $\mathbb{R}^n$ defined by the equality constraints $F_1 = 0, \ldots, F_p = 0$.
Let G and $F_1, \ldots, F_p \in \mathbb{Q}[X_1, \ldots, X_n]$ be given as outputs of an essentially division–free arithmetic circuit β in $\mathbb{Q}$ having size L. Let $d \geq 2$ be an upper bound for $\deg G, \deg F_1, \ldots, \deg F_p$.

3.2.1 Minimal point searching problems

We first consider the problem of finding all isolated local minimal points of G in $V_{\mathbb{R}} = \{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$. For this purpose we search for every index sequence $1 \leq j_1 < \cdots < j_p \leq n$ the isolated local minimal points of G in the corresponding chart $(V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$. Let $\delta_{j_1,\ldots,j_p}$ be the maximal degree of the Zariski closures in $\mathbb{C}^n$ of all locally closed sets

$$\{F_1 = 0, \ldots, F_j = 0\}_{\Delta_{j_1,\ldots,j_p} \cdot \det H_{j_1,\ldots,j_p}}, \quad 1 \leq j \leq p, \quad \text{and}$$
$$\{F_1 = 0, \ldots, F_p = 0,\ M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}_{\Delta_{j_1,\ldots,j_p} \cdot \det H_{j_1,\ldots,j_p}},\ 1 \leq k \leq n-p,$$

where $H_{j_1,\ldots,j_p}$ is the Hessian matrix of G on $V_{\Delta_{i_1,\ldots,j_p}}$.
Let finally

$$\delta := \max\{\delta_{j_1,\ldots,j_p} \mid 1 \leq j_1 < \cdots < j_p \leq n\}.$$

We call δ the *degree* of the isolated minimum searching problem for G on $V_{\mathbb{R}} = \{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$. From the Bézout Inequality we deduce

$$\delta \leq ((p+1)\,d)^n = (n\,d)^{O(n)}.$$

Fix now $1 \leq j_1 < \cdots < j_p \leq n$ and observe that $W_{\Delta_{j_1,\ldots,j_p} \cdot \det H_{j_1,\ldots,j_p}}$ is empty or a zero-dimensional variety. Hence, for $1 \leq k < n-p$ no irreducible component of the variety

$$\{F_1 = 0, \ldots, F_p = 0,\ M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}_{\Delta_{j_1,\ldots,j_p} \cdot \det H_{j_1,\ldots,j_p}}$$

is contained in $W_{\Delta_{j_1,\ldots,j_p} \cdot \det H_{j_1,\ldots,j_p}}$. In the same way as in the proof of Lemma 6 we conclude now that $F_1, \ldots, F_p, M_1^{(j_1,\ldots,j_p)}, \ \ldots, M_k^{(j_1,\ldots,j_p)}$ generate the trivial ideal or form a reduced regular sequence in $\mathbb{R}[X_1, \ldots, X_n]_{\Delta_{j_1,\ldots,j_p} \cdot \det H_{j_1,\ldots,j_p}}$.

Applying now the Kronecker algorithm [20] to the input system

$$F_1 = 0, \ldots, F_p = 0,\ M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_{n-p}^{(j_1,\ldots,j_p)} = 0,\ \ \Delta_{j_1,\ldots,j_p} \cdot \det H_{j_1,\ldots,j_p} \neq 0$$

represented by the circuit β we obtain for the at most $\delta_{j_1,\ldots,j_p}$ complex points of $\{F_1 = 0, \ldots, F_p = 0,\ M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_{n-p}^{(j_1,\ldots,j_p)} = 0\}_{\Delta_{j_1,\ldots,j_p} \cdot \det H_{j_1,\ldots,j_p}}$ an algebraic description over $\mathbb{Q}$. For the real points among them we obtain even a description à la Thom. We now discard the points with non-zero imaginary part and evaluate the signature of the Hessian matrix $H_{j_1,\ldots,j_p}$ at each of the real points and discard the real points where the Hessian is not positive definite. The remaining real points are by Lemma 7 exactly the isolated local minimal points of G in $(V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}}$. Repeating this procedure for each $1 \leq j_1 < \cdots < j_p \leq n$ we obtain all isolated local minimal points of G in $V_{\mathbb{R}}$.

The complexity analysis of [20] yields a time bound of $L \binom{n}{p}\ (n\,d)^{O(1)}\,\delta^2 = (n\,d)^{O(n)}$ for the whole procedure. Combining the Binet–Cauchy formula [17] with a similar argumentation as in the proof of [28] Theorem 4.4, one can show that one may find probabilistically regular matrices $A_1, \ldots, A_{n-p+1} \in \mathbb{Z}^{n \times n}$ of logarithmic heights $O(n \log dn)$ and p–minors $\mathbf{\Delta}_1, \ldots, \mathbf{\Delta}_{n-p+1}$ of $J(F_1, \ldots, F_p) \cdot A_1, \ldots, J(F_1, \ldots, F_p) \cdot A_{n-p+1}$ such that $V_{\mathbf{\Delta}_1} \cup \cdots \cup V_{\mathbf{\Delta}_{n-p+1}}$ is the regular locus of V (see [6] for details). Thus we may improve the sequential bound above to $L\,(n\,d)^{O(1)}\,\delta^2$.

Theorem 12
Let $n, d, p, L, \ell, \delta \in \mathbb{N}$ with $1 \leq p \leq n$ be arbitrary and let $G, F_1, \ldots, F_s \in \mathbb{Q}[X_1, \ldots, X_n]$ be polynomials of degree at most d satisfying Conditions B and C and having isolated local minimum searching degree at most δ. Suppose that $G, F_1, \ldots, F_s$ are given as outputs of an essentially division-free circuit β in $\mathbb{Q}[X_1, \ldots, X_n]$ of size L.

There exists a uniform bounded error probabilistic algorithm $\mathcal{B}$ over $\mathbb{Q}$ which computes from the input β in time $L\,(nd)^{O(1)}\delta^2 = (nd)^{O(n)}$ all isolated local minimal points of G in $V_{\mathbb{R}} = \{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$.

For any $n, d, p, L, \ell, \delta \in \mathbb{N}$ with $1 \leq p \leq n$ the probabilistic algorithm $\mathcal{B}$ may be realized by an algebraic computation tree of depth $L\,(n\,d)^{O(1)}\,\delta^2 = (n\,d)^{O(n)}$ that depends on parameters which may be chosen randomly.

Let us now consider the problem of searching for the isolated local minimal points in the case of unconstrained optimization. Let H be the Hessian matrix of G. Observe that Conditions E and F imply that the polynomials $\frac{\partial G}{\partial X_1}, \ldots, \frac{\partial G}{\partial X_n}$ generate the trivial ideal or form a reduced regular sequence in $\mathbb{Q}[X_1, \ldots, X_n]_{\det H}$. Let δ be the maximal degree of the Zariski closure in $\mathbb{C}^n$ of the locally closed sets $\{\frac{\partial G}{\partial X_1} = 0, \ldots, \frac{\partial G}{\partial X_n} = 0\}_{\det H}$, $1 \leq k \leq n$. We call δ the *degree* of the isolated minimum searching problem for G on $\mathbb{R}^n$. The Bézout inequality implies $\delta \leq (d-1)^n \leq d^n$. Applying the Kronecker algorithm to the input system

$$\frac{\partial G}{\partial X_1} = 0, \ldots, \frac{\partial G}{\partial X_n} = 0, \;\; \det H \neq 0$$

we obtain the analogous statement of Theorem 12 for the isolated minimum searching problem in the unconstrained case.

The aim of the next algorithm is to compute a real algebraic point which is a global minimal point of G in $V_{\mathbb{R}} = \{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$ if there exists one. For this purpose we construct for each $1 \leq j_1 < \cdots < j_p \leq n$ and each $1 \leq k \leq n-p$ suitable real algebraic sample points of

$$(V_{\mathbb{R}})_{\Delta_{j_1,\ldots,j_p}} \cap \{M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}_{\mathbb{R}} \setminus (D_k)_{\mathbb{R}}.$$

Let x be a minimal point of G in $V_{\mathbb{R}}$ and let $a := G(x)$. Then x belongs to W and therefore there exists by Lemma 5 an irreducible component of W where G takes only the value a. This fact will guarantee that we are able to find a minimum of G on $V_{\mathbb{R}}$. For $1 \leq j_1 < \cdots < j_p \leq n$ and $1 \leq k \leq n-p$ let $\delta_{j_1,\ldots,j_p;k}$ be the maximal degree of the Zariski closures in $\mathbb{C}^n$ of all locally closed sets

$$\{F_1 = 0, \ldots, F_j = 0\}_{\Delta_{j_1,\ldots,j_p} \cdot R_k}, \;\; 1 \leq j \leq p, \;\; \text{and}$$
$$\{F_1 = 0, \ldots, F_p = 0,\, M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_{k'}^{(j_1,\ldots,j_p)} = 0\}_{\Delta_{j_1,\ldots,j_p} \cdot R_k},\; 1 \leq k' \leq k$$

and all generic dual polar varieties of

$$\{F_1 = 0, \ldots, F_p = 0,\, M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}_{R_k}$$

(take Lemma 6 into account). Let finally

$$\delta := \max\{\delta_{j_1,\ldots,j_p;k} \mid 1 \leq j_1 < \cdots < j_p \leq n,\; 1 \leq k \leq n-p\}$$

We call δ the *degree* of the global minimum searching problem for G on $V_{\mathbb{R}}$. From the Bézout inequality we deduce

$$\delta \leq (n(p+1)d)^n = (n\,d)^{O(n)}.$$

We construct now recursively in $1 \leq k \leq n-p$ an ascending chain of finite sets Y_k of real algebraic points of $V_{\mathbb{R}}$ such that $G(Y_k)$ contains the set B_{k+1} (see Subsection 3.1 for the definition of B_{k+1}).

In order to construct Y_1 we apply the algorithm [2, 3] to the system $F_1 = \cdots = F_p = 0$. The algorithm returns a finite set Y_1 of algebraic points of $V_{\mathbb{R}}$.

Let now $2 \leq k \leq n-p$ and suppose that we have already constructed Y_{k-1} subject to the condition $B_k \subset G(Y_{k-1})$.
Let $\widetilde{R}_k := \prod_{y \in Y_{k-1}} (G - G(y))$ and observe that $\widetilde{R}_k$ is a multiple of R_k in $\mathbb{R}[X_1, \ldots, X_n]$.
Taking into account Lemma 6 and that $\widetilde{R}_k$ is a multiple of R_k we apply now the same algorithm to the system

$$F_1 = 0, \ldots, F_p = 0,\ M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0, \widetilde{R}_k \neq 0.$$

In this way we obtain finitely many algebraic points of $V_{\mathbb{R}}$ which together with Y_{k-1} form Y_k.
Let us consider an arbitrary irreducible component C of W of dimension $n-p-k$ on which, by virtue of Lemma 5, the constant value of G does not belong to $G(Y_{k-1})$. Then we have $C_{\widetilde{R}_k} = C$ and therefore C and $C_{\mathbb{R}}$ are contained in

$$\{F_1 = 0, \ldots, F_p = 0,\ M_1^{(j_1,\ldots,j_p)} = 0, \ldots, M_k^{(j_1,\ldots,j_p)} = 0\}_{\widetilde{R}_k}$$

Hence, by [4], Theorem 1 the generic dual polar varieties of this locally closed set are not empty and the $(n-p-k)$th one contains a point of $C_{\mathbb{R}}$. Applying this argument inductively we see that $G(W) \subset G(Y_{n-p})$ holds. We suppose now that G reaches a global minimum on $\{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$. Then Y_{n-p} must contain a global minimal point of G in $V_{\mathbb{R}} = \{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$ which is an element, say y, of Y_{n-p} with $G(y) = \min_{x \in Y_{n-p}} G(x)$.

The complexity analysis of the algorithm of [2, 3] yields a time bound of $L\binom{n}{p} 2^{n-p} (n\,d)^{O(1)} \delta^2 = (n\,d)^{O(n)}$ for the whole procedure. We may use the same argumentation as before Theorem 12 in order to improve this bound to $L\,(n\,d)^{O(1)}\,\delta^2$. We obtain now the following complexity result.

Theorem 13
Let n, d, p, L, ℓ, $\delta \in \mathbb{N}$ with $1 \leq p \leq n$ be arbitrary and let $G, F_1, \ldots, F_s \in \mathbb{Q}[X_1, \ldots, X_n]$ be polynomials of degree at most d satisfying Conditions B, C and D and having global minimum searching degree at most δ. Suppose that $G, F_1, \ldots, F_s$ are given as outputs of an essentially division-free circuit β in $\mathbb{Q}[X_1, \ldots, X_n]$ of size L.

There exists a uniform bounded error probabilistic algorithm $\mathcal{C}$ over $\mathbb{Q}$ which computes from the input β in time $L\,(nd)^{O(1)}\,\delta^2 = (nd)^{O(n)}$ a global minimal point of G in $V_{\mathbb{R}} = \{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$ if there exists one.

For any n, d, p, L, ℓ, $\delta \in \mathbb{N}$ with $1 \leq p \leq n$ the probabilistic algorithm $\mathcal{C}$ may be realized by an algebraic computation tree of depth $L\,(nd)^{O(1)}\delta^2 = (nd)^{O(n)}$ that depends on parameters which may be chosen randomly.

Mutatis mutandis the same statement is true for the unconstrained optimization problem. The degree of the minimum searching problem in this case is the maximal degree

of the Zariski closures in $\mathbb{C}^n$ of all locally closed sets $\{\frac{\partial G}{\partial X_1}, \ldots, \frac{\partial G}{\partial X_k}\}_{R_k}$, $1 \leq k \leq n$ and all generic dual polar varieties of them.

The reader should observe that Theorem 13 does not answer the question whether G reaches a global minimum on $\{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$ and can only be applied when this existence problem is already solved. For this problem we refer to [22].

4 Conclusion

Together with [31] this paper represents only a first attempt to introduce the viewpoint of intrinsic quasi–polynomial complexity to the field of polynomial optimization. For this purpose we used some restrictive conditions which allow us to apply our algorithmic tools. In the future we shall relax these restrictions and extend the algorithmic tools and the list of real problems which can be treated in this way.

References

[1] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop, Polar varieties and efficient real elimination, Math. Z. 238 (2001), 115-144.

[2] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo, Generalized polar varieties and an efficient real elimination procedure, Kybernetika 40 (2004), 519-550.

[3] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo, Generalized polar varieties: geometry and algorithms, J. Complexity 21 (2005), 377-412.

[4] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and E. Schost, On the geometry of polar varieties, Appl. Algebra Eng. Commun. Comput. 21 (2010), 33-83.

[5] B. Bank, M. Giusti, and J. Heintz, Point searching in real singular complete intersection varieties - algorithms of intrinsic complexity, 2012 accepted by Math. Comp.

[6] B.Bank, M. Giusti, J.Heintz, G. Lecerf, G. Matera, and P. Solernó, Degeneracy loci and polynomial equation solving, Manuscript, Universidad de Buenos Aires, 2013.

[7] S. Basu, R. Pollack, and M.-F. Roy, On the combinatorial and algebraic complexity of quantifier elimination, J.ACM 43 (1996), 1002-1045.

[8] S. Basu, R. Pollack, and M.-F. Roy, Algorithms in real algebraic geometry, (2nd ed.). Springer Verlag, Berlin etc., 2006.

[9] J. Bochnak, M. Coste, and M.-F. Roy, Géométrie algébrique réelle, Springer Verlag, Berlin etc. 1987.

[10] P. Bürgisser, M. Clausen, and M. A. Shokrollahi, Algebraic complexity theory, with the collaboration of Thomas Lickteig, Grundlehren der Mathematischen Wissenschaften 315, Springer Verlag, Berlin etc., 1997.

[11] A. Cafure, and G. Matera, Fast computation of a rational point of a variety over a finite field, Math. Comput. 75 (2006), 2049–2085.

[12] J.F. Canny, Some algebraic and geometric computations in PSPACE, ACM Symposium on Theory of Computing (STOC), 1988, 460-467.

[13] M. Coste and M.-F. Roy, Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets, J. Symb. Comput. 5 (1988), 121-129.

[14] M. Demazure, Catastrophes et bifurcations, Ellipses, Paris, 1989.

[15] C. Durvye and G. Lecerf, A concise proof of the Kronecker polynomial system solver from scratch, Expo. Math. 26 (2008), 101-139.

[16] W. Fulton, Intersection theory (2nd ed.), Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge 2, Springer Verlag, Berlin etc., 1998.

[17] F. R. Gantmacher, Théorie des matrices. I: Théorie générale. II: Questions speciales et applications, Dunod, Paris (1966).

[18] M. Giusti, J. Heintz, K. Hägele, J. E. Morais, J. L. Montaña, and L.M. Pardo, Lower bounds for diophantine approximations, J. Pure Appl. Algebra 117-118 (1997), 277-317.

[19] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, and L.M. Pardo: Straight–line programs in geometric elimination theory, J. Pure Appl. Algebra 124 (1998), 101-146.

[20] M. Giusti, G. Lecerf, and B. Salvy, A Gröbner free alternative for polynomial system solving, J. Complexity 17 (2001), 154-211.

[21] A. Greuet, Optimisation globale algébrique et variétés: théorie, algorithmes et implantations, PhD thesis, Université Versailles Saint-Quentin, 2013.

[22] A. Greuet and M. Safey El Din, Deciding reachability of the infimum of a multivariate polynomial, ISSAC 2011 Proceedings, San Jose, 2011.

[23] A. Greuet, F. Guo, M. Safey El Din, L. Zhi, Global optimization of polynomials restricted to a smooth variety using sums of squares, J. Symb. Comput. 47 (2012) 883–901.

[24] D. Grigor'ev and N. Vorobjov, Solving systems of polynomial inequalities in subexponential time, J. Symb. Comput. 5 (1988), 37-64.

[25] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theor. Comput. Sci. 24 (1983), 239-277.

[26] J. Heintz, G. Matera, and A. Waissbein, On the time-space complexity of geometric elimination procedures, Appl. Algebra Eng. Commun. Comput. 11 (2001), 239-296.

[27] J. Heintz, M.-F. Roy, and P. Solernó, On the complexity of semialgebraic sets, in IFIP Information Processing 89 (G. X. Ritter , ed.), Elsevier, 1989, pp. 293-298.

[28] J. Heintz, and C. P. Schnorr, Testing polynomials which are easy to compute, Logic and algorithmic, Int. Symp., Zürich 1980, Monogr. L'Enseign. Math. 30, (1982) 237-254.

[29] G. Jeronimo, D. Perrucci, and E. Tsigaridas, On the minimum of a polynomial function on a basic closed semialgebraic set and applications, (2011) to appear in Siam J. of Optimization.

[30] G. Lecerf, Kronecker software package,
http://www.math.uvsq.fr/∼lecerf/software/index.html

[31] C. Le Guernic, and M. Safey El Din, On the practical computation of one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and non-strict inequalities, INRIA Rapport de recherche 5079 (2004) and in (L. Gonzalez-Vega, ed.) Proceedings of EACA, Santander, Spain (2004).

[32] D. Mumford, The red book of varieties and schemes, Lecture Notes in Mathematics, 1358. Berlin etc., Springer-Verlag, 1988

[33] H. Matsumura, Commutative ring theory, (transl. from the Japanese by M. Reid), Paperback Cambridge Studies in Advanced Mathematics, 8. Cambridge etc., Cambridge University Press, 1989.

[34] J. Renegar, A faster PSPACE algorithm for the existential theory of the reals, in Proc. 29th Annual IEEE Symposium on the Foundation of Computer Science, 1988, pp. 291-295.

[35] J. Renegar, On the computational complexity and geometry of the first order theory of the reals, J. Symb. Comput.,13 (1992), 255-352.

[36] M. Safey El Din and E. Schost, Polar varieties and computation of one point in each connected component of a smooth real algebraic set, in Proc. ISSAC 2003, J. R. Sendra, ed., ACM Press, 2003, pp. 224–231.

[37] M. Safey El Din, Computing the global optimum of a multivariate polynomial over the reals, ISSAC 2008 Proceedings, D. Jeffrey (eds), Austria (Hagenberg), 2008.

[38] M. Safey El Din, Practical and theoretical issues for the computation of generalized critical values of a polynomial mapping, in (D. Kapur ed.) ASCM 2007, Lecture Notes in Computer Science 5081, Berlin, Springer, 2008.

[39] Igor R. Shafarevich, Basic algebraic geometry. 1: Varieties in projective space, Springer Verlag, Berlin, 1994.

[40] W. Vogel, Lectures on results on Bézout's theorem. Notes by D. P. Patil, Lectures on Mathematics and Physics, Mathematics, 74, Tata Institute of Fundamental Research, Springer Verlag, Berlin etc.,1984.